

POSITION STATEMENT

1. POSITION INFORMATION	
CIVIL SERVICE CLASSIFICATION:	WORKING TITLE:
Information Technology Specialist I	<i>Information Security Analyst</i>
NAME OF INCUMBENT:	POSITION NUMBER:
	280-390-1402-006
OFFICE/SECTION/UNIT:	SUPERVISOR'S NAME:
Privacy & Integrated Risk Management Office/Security Policy & Compliance Unit	
DIVISION:	SUPERVISOR'S CLASSIFICATION:
Cybersecurity Division	Information Technology Manager I
BRANCH:	REVISION DATE:
Information Technology Branch	5/15/2025
Duties Based on: <input type="checkbox"/> FT <input type="checkbox"/> PT– Fraction _____ <input type="checkbox"/> INT <input type="checkbox"/> Temporary – _____ hours	
2. REQUIREMENTS OF POSITION	
Check all that apply: <input checked="" type="checkbox"/> Conflict of Interest Filing (Form 700) Required <input type="checkbox"/> Call Center/Counter Environment <input type="checkbox"/> May be Required to Work in Multiple Locations <input checked="" type="checkbox"/> Requires Fingerprinting & Background Check <input type="checkbox"/> Requires DMV Pull Notice <input type="checkbox"/> Bilingual Fluency (<i>specify below in Description</i>) <input type="checkbox"/> Travel May be Required <input type="checkbox"/> Other (<i>specify below in Description</i>)	
Description of Position Requirements: (e.g., qualified Veteran, Class C driver's license, bilingual, frequent travel, graveyard/swing shift, etc.)	
<div style="border: 1px solid black; height: 30px;"></div>	
3. DUTIES AND RESPONSIBILITIES OF POSITION	
Summary Statement: (Briefly describe the position's organizational setting and major functions)	
Information Technology Domains (Select all domains applicable to the incumbent's duties/tasks.) <input checked="" type="checkbox"/> Business Technology Management <input checked="" type="checkbox"/> IT Project Management <input type="checkbox"/> Client Services <input checked="" type="checkbox"/> Information Security Engineering <input type="checkbox"/> Software Engineering <input type="checkbox"/> System Engineering	
<p>Under the direction of the Information Technology Manager I, the Information Security Analyst performs complex and sensitive tasks in support of the Cybersecurity Division. The incumbent leads the efforts to develop, review, and update information security policies, standards, procedures, and information technology circulars.</p> <p>The incumbent serves as a subject matter expert (SME) of the California Cybersecurity Maturity Metrics, as defined by SIMM 5300-C, to ensure EDD alignment with the five security domains (Identify, Protect, Detect, Respond, and Recover).</p>	

The incumbent performs impact analysis by tracking and providing ongoing review and updates of policy and standards, risk assessments, business and privacy assessments, and the reporting requirements needed to fulfill mandated compliance.

The incumbent provides guidance and assistance as needed in support of the other lines of business within the Privacy and Risk Management Unit. Architects reusable, effective and innovative SharePoint solutions, configures and manages Cybersecurity SharePoint sites. Designs and implements permission strategies for security and technology audiences. Works with users to identify requirements, train on usage, and troubleshoot more complex problems.

The incumbent also contributes toward the growth of the Information Technology Branch into a customer-focused, service organization by following Branch cultural principles and by providing constructive feedback to others within the Branch regarding the application of those principles.

Percentage of Duties	Essential Functions
40%	Develops, researches, documents, and maintains policies, procedures, and standards for Information Security related items with guiding influence derived from National Institute of Standards and Technology (NIST), Statewide Information Management Manual (SIMM), and the State Administration Manual (SAM). Works with subject matter experts, designated reviewers and approvers to develop and update policies, processes, procedures, and standards on an annual basis.
20%	Assists with independent Business and/or Privacy Impact Analyses to define and assess the potential impact to the organization as a result of various projects in flight, as well as security incidents causing disruption of service or major outages. Utilizes software reporting applications such as the GRC (Governance/Risk/Compliance) tool to provide mandated reporting updates as needed for enterprise applications / systems.
15%	Provides information security oversight and compliance reviews for new/existing projects. Works closely with business, technical and project teams during the Project Approval Lifecycle, the CA-Project Management Framework, the Service Delivery Discipline and the Software Development Lifecycle processes through monitoring, reviews and application of IT security policies, standards, procedures and guidelines in support of the EDD Information Security Office (ISO) Lines of Businesses (LOBs).
10%	Assists with the development and maintenance of the Cybersecurity Division SharePoint sites. Works with Cybersecurity Division staff to identify requirements for the creation of additional SharePoint sites and applications, trains staff on Cybersecurity Division SharePoint sites and usage.
10%	Assists with the development and maintenance of the security-related training and awareness materials such as training modules, educational posters, phishing campaigns and other associated training requirements.

Civil Service Classification
Information Technology Specialist I

Position Number
280-390-1402-006

Supervisor: After signatures are obtained, make 2 copies:

- Send a copy to HRSD (via your Attendance Clerk) to file in the employee's Official Personnel File (OPF)
- Provide a copy to the employee
- File original in the supervisor's drop file